UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
V.	)	No. 16-10305-NMG
MARTIN GOTTESFELD,	)	
Defendant	)	

DEFENDANT'S SUPPLEMENTAL MOTION TO SUPPRESS AND REQUEST FOR EVIDENTIARY HEARING

Introduction

Defendant Martin Gottesfeld, by his undersigned attorney, hereby supplements his previously filed motion to suppress evidence (hereafter "Suppression") obtained from the execution of a search warrant on October 1, 2014 at his Somerville apartment. In particular, he supplements that part of the motion attacking the results of the Pen Register/Trap and Trace order ("Pen/Trap") which underpinned the finding of probable cause for issuance of the search warrant. The original motion argues two bases for suppression. First, that the electronic surveillance for 60 days 24 hours a day constituted such a prolonged invasion of privacy, cataloging defendant's daily activities, interests, likes and dislikes, as he traveled on the Internet, that it violates the Fourth Amendment, analogizing to the vehicle tracking device sharply criticized by five concurring justices in United States v. Jones, 132 S.Ct. 945, 954, 964 (2012), Suppression, at 5-6; and, second, that the identification of destination Internet Protocol ("IP")

addresses (with subscriber information) illegally seized "content" in violation of § 3127(3) - (4) of the Pen /Trap Act. 18 U.S.C. §§ 3121 – 3127 and, as such, was a violation of his reasonable expectation of privacy in the contents of his online communications akin to the contents of the phone conversation in a public telephone booth first enunciated in Katz v. United States, 389 U.S. 347 (1967). Id. at 6-7. Just as the use of a public, coin-operated, telephone behind a closed door implied an expectation of privacy in Katz , so defendant's use of the anonymizing Internet router/browser, The Onion Router, "TOR", evinced an equally valid expectation of privacy. Id. 7-8.

This supplement further details the argument regarding the illegal seizure of IP addresses and adds two new arguments.

First, the capture of internet port numbers was also a violation of § 3127(3) - (4) because ports as well as IP addresses contain content that has "substance, purport, or meaning". Collectively they can also yield an extensive profile of one's daily activities and interests. Ports warrant a stronger inference of an expectation of privacy in their content than do IP addresses. The communication from source port to destination port is a direct end-to-end, or, better said, host- to-host, transfer with no inspection by third parties along the way.

Second, the search warrant on its face does not demonstrate probable cause and the only explanation for its issuance appears to be an unacknowledged bias and conflict of interest on the part of the issuing magistrate judge. She was not a detached, independent, or neutral arbiter. She actually had close ties, both financial and personal, to the victim, Boston Childrens' Hospital, of the DDOS attack alleged in the present indictment. This obvious conflict of interest should have been disclosed and the magistrate should have recused herself from hearing the search warrant

application by the government. The failure to do that has two ramifications at this time. The probable cause finding was tainted, and there should be no good faith exception to the exclusionary rule in the present case.

Factual Background

Defendant respectfully directs the Court's attention to the recitation of facts contained in the original motion to suppress in the "Background" section. He also adds the following: even his expert's review of just a tiny portion of the 248 spreadsheets of traffic produced from the pen/trap permits the creation of a quite detailed portrait of the defendant based solely on the capture of IP addresses. See Exhibit A, attached. Professor Ciaraldi states the following:

"Looking at a user's Internet traffic, and just looking at the IP addresses, reveals enough information to form a rather detailed profile of the user. For example, in a 25 hour period (August 18-19, 2014) Gottesfeld accessed approximately 740 different IP addresses. I was able to identify DNS (Domain Name Service) names for 490 of them, including the following:

> Span.com: Maker of high-end computer storage software.
> Canonical.com: Provider of Ubuntu, a Linux operating system distribution.
> Mozilla.com: Makers of the Firefox web browser.
> nagios.org: Provider of sophisticated software for managing computers and other networked devices.
> Newrelic.com: Site for technical computer and gadget news.
> Yahoo.com: General Internet news site.
> Gazeta.pl: A Polish newspaper.
> 1e100.net: Google, reportedly related to its YouTube service.
> Facebook.com: Social media site (this IP address was specifically for Facebook in Ireland).
>
> One can draw the conclusion that the user is almost certainly a computer professional, likely a networking specialist. For example, the hardware made by Span is professional grade, beyond what all but the most advance hobbyists would use. Similarly, Nagios is a very complex software package used for managing multiple computers, routers, and other networked devices. Since the user accessed gazeta.pl it is reasonable to conclude that he reads the Polish language and is interested in news from

Poland."

One can draw the conclusion that the user is almost certainly a computer professional. For example, the hardware made by Span is professional grade, beyond what all but the most advanced hobbyists would use. Similarly, Nagios is a very complex software package used for managing multiple computers, routers, and other networked devices."

Exhibit A.

Statutory Framework

The Pen/Trap act defines a pen register as "a device or process which records or decodes dialing, routing, addressing or signaling information". Id. § 3127(3). A trap and trace device is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing and signaling information reasonably likely to identify the source of a wire or electronic communication". Id. § 3127(4). But in both instances, "such information shall not include the contents of any communication". Id. §§ 3127(3) & (4). Content is defined as, "any information concerning the substance, purport or meaning of that communication." 18 U.S.C. § 3721(1) and §2510 (8).

Application to Port Captures

The Pen/Trap Act was passed in 1986. Pub. L. 99-508, title III, § 301(a), Oct. 21, 1986, 100 Stat. 1868. Popular usage of the Internet was in its infancy at the time. The Act was "exclusively focused on the telephony world." [1] Dialing, routing, addressing, or signaling information may have been only metadata without "content" in 1986 but in the Internet of today sometimes it can, in fact, be content.

1 See Bellovin, et al., "It's Too Complicated: How the Internet Upends *Katz*, *Smith* and Electronic Surveillance Law", Harvard Journal of Law & Technology, Vol. 30, Number 1, Fall 2016, n. 12, p. 4. "Bellovin, et al." Available online at https://www.lawfareblog.com/its-too-complicated-how-internet-upends-katz-smith-and-electronic-surveillance-law.

> "The examination of these examples suggests that the content/non-content distinction erodes or collapses in three primary ways: (1) some information fits into neither statutory definition; (2) depending on where in the network one asks the question, *content may be architectural content for one party and* architectural metadata or *communicative content for another*; and (3) extremely revelatory information may nevertheless fail to satisfy the statutory definition of content, and thus cannot claim the privacy protections afforded content under statutory law." [2] (Emphases supplied).

Defendant asserts that port information can, in fact, be the equivalent of content under the statute. "A "port" is a piece of information used to identify the purpose of a particular packet of data being transferred between computers [on the Internet]". See PC Magazine, *Definition of TCP/IP Port* <tinyurl.com/portdefinition> (last accessed December 22, 2017). Ports represent the types of transmission being made. Many of the more often-used ports are easily recognizable by anyone familiar with Transmission Control Protocol/Internet Protocol ("TCP/IP") For example, port numbers "80" and "443" indicate transmission to a server on the World Wide Web. Numbers "25", "110" or "143" denote email traffic. Port transmission numbers can also be looked up on various free online services. See e.g. https://en.wikipedia.org/wiki/ List_of_TCP_and_UDP_port_numbers. For example, port number 23399 is used for Skyping.

Initial Results of Traffic Review

Brief Technical Introduction.

Communication on the Internet is transmitted by packets of information. These packets consist of "headers" and "payloads". There can be multiple layers of headers. The Internet Protocol ("IP") header contains the IP address. It tells the routers comprising the Internet where to send the packets. Within the payload is another header, typically either TCP (Transmission Control Protocol) or UDP (User Datagram Protocol). This is where the port number is stored,

2 Bellovin, supra at 53.

and is used to direct the packet once it reaches the host computer at the destination IP address. The system determines which application should process the packets based on the TCP or UDP port number. Port numbers facilitate the delineation of packets from different applications, and are not examined in transit for routing or addressing. Thus, it is called an "end-to- end" transmission. Internet Protocol or "IP" addresses, on the other hand, must be examined along the way to facilitate speed and accuracy.

The Pen/Trap devices in this case captured four pieces of information for each connection that defendant's computer made on the Internet: source port number and IP address and destination port number and IP address. They also recorded the date, time and duration of the connections.

Limits of Expert Review to Date

In discovery, the government has produced 248 Excel spreadsheets each with approximately 10,000 lines of data detailing the source and destination ports and IP addresses of defendant's computer traffic during the 60 days permitted by the court order. Defendant's expert has only been able to review a small fraction of those entries as of the date hereof. Nevertheless, his collection and analysis of just a relatively small sample of traffic demonstrates that port numbers do convey "substance, purport, or meaning".

For example, he found numerous instances of connections to web servers by the indicated source ports of 80 and 443. There were connections on port 161 which indicates access to SNMP, or Simple Network Management Protocol, and connections using port 22 which is used for SSH or Secure Shell which is used for remote access to another computer on the Internet. Port numbers 25, 465, and 587 refer to outgoing non-web based email. Non-web incoming email

uses ports 109, 110, 993 or 995. Web-based email uses regular web site ports, i.e. 80 and 443. Gmail.com is an example of a web-based email service.

Various on-line video games have identifiable port numbers. The popular Minecraft game uses ports 25565 and 25575. Different versions of Quake use ports 7133 (enemy territory: Quake Wars), 26000 (Central Quake server), 27000-27006 (QuakeWorld), 27500-27900 (QuakeWorld), 27901-27910 (Quake II) and 27960-27969 (QuakeIII and Quake Live and Quake III Arena). Windows Media Center on a Microsoft Windows operating system can record television programs running on the Internet. A port number 5832 on an incoming connection means the user is accessing the recorder remotely. Securedserver.net is a Virtual Private Network ("VPN") server. Users who access it via port 1194 can establish a private, password – required, encrypted end-to-end network connection between their computer and a single website without any intermediary switching. Godaddy.com is another example that also permits VPN networking. The TOR (The Onion Router) browser is a free, encrypted, internet router service which provides anonymous browsing. [3]

Sample Profile Creation

Using just the port numbers identified above and running them through either an online index or doing a reverse search from a DOS command prompt would allow one to create a meaningful profile of the person sitting at the computer traversing the Internet.

For example, seeing the incoming port numbers 109, 110, 993 and 995 in the early morning would indicate the use of a private application, non-web based email service. Subsequent destination ports 80, or 443 would indicate visits to web sites. A change to

3 The government has alleged that the defendant was using both a VPN and TOR, as 'potentially indicative' of criminal intent. See Affidavit, Ex. A to Suppression, at ¶ ¶ 22-26.

destination port number 161, especially for a prolonged period, would indicate access to tools for SNMP, or Simple Network Management Protocol, and, depending on the actual IP address visited and the length thereof, could indicate amateur tinkering or professional level technical work. A flurry of traffic to port 53 indicates a visit to DNS, the domain name service, which functions as a kind of telephone directory for the Internet, identifying entities using a particular IP address or vice versa using a reverse search query. An hour at mid-day divided by two with half that time at port 25565 or 25575 and the other at port 7133 would likely indicate that at his/her lunch break the user played the online video games Minecraft and Quake Wars: Enemy Territory, in succession.

Intermittent use of a web-based email for communications with off-site personnel could indicate casual contacts. But if there was ongoing evidence of prolonged connection to port 22, used for SSH (Secure Shell) to make a remote connection to another computer, that could readily be interpreted as formal employment by remote connection from one's own residence. Such a connection would allow an employee to work from home by typing commands and running his office programs from his home location. Long periods of after-dinner time showing incoming traffic on port 5832 means that the user is not at home. Instead he is somewhere else using an app on his smart phone to record selected TV programs by accessing Windows Media Center on his home computer.

Some of the foregoing profile is based on an analysis of a very small amount, approximately 4 %, of traffic data captured by the Pen/Trap in this case. The raw information was provided by defendant's expert and the interpretation by the undersigned after vetting by the expert. The resulting hypothetical user portrait, admittedly done in broad strokes more than

pointillist detail, merely hints at the interpretive potential of a much larger sample. That potential could be greatly expanded by employing a computer program instead of a person to perform the remaining review. See e.g. American Civil Liberties Union, et al. v. Clapper, 785 F/3d 787, 794 (2d Cir. 2014)("But the structured format of telephone and *other technologically-related metadata, and the vast new technological capacity for large-scale and automated review and analysis,* distinguish the type of metadata at issue here from more traditional forms.") (*italics supplied).* The point is that evolving technology makes the interpretation of port numbers, and especially in the context of the possible temporal sequences in which they occur, much more likely to reveal information more akin to content that reveals "significance, purport or meaning" then to mere "dialing, routing, addressing or signaling information." [4]

Argument

I. The Constant Real Time Surveillance for 60 Days, 24 Hours a Day of that Part of Defendant's Internet Traffic Which Included Port Numbers Violated His Rights Under the Fourth Amendment.

As defendant has argued in his initial motion to suppress, without evidence of his usage of TOR and the VPN, insuring anonymity and privacy, respectively, the affidavit in support of the application for the search warrant does not demonstrate probable cause. **Suppression**, at 15. In addition, he says that the Pen/Trap captured "content" which the statute, 18 U.S.C. § 3127(3)(4), expressly prohibits. The motion focuses only on the IP addresses as containing content. **Id.** at ____. Here he adds another basis for finding that the Pen/Trap obtained illegal content information: the access to port numbers for each and every trip that he took during his Internet surfing.

4 There are many more port numbers assigned to a specific website, company or type of traffic. See e.g. Exh. B.

Legal Framework

The "Third Party Doctrine" Has no Reasonable Application to Port Numbers.[5] This is because the information conveyed by a port number is not made available to any third party. The Internet is significantly different from the old wired telephone network.

As described by Bellovin, et al. **supra**, n. 1,

> "The transport layer, which is responsible for delivery of data to applications, is strictly end-to-end. The contents of the TCP ["Transmission Control Protocol"] are created by one end system and are relevant only to the peer TCP at the other end of the connection. Unlike the network layer, intermediate routers do not examine or otherwise rely on TCP. In other words, the data transmitted between peer TCP, is not, from an Internet design perspective, shared with other parties. … [and]
>
> "Unlike in the phone system; these headers are end-to-end; they are not processed by the network."
>
> Bellovin, et al. 42.

TCP contains port numbers. Id.[6] The Smith third- party rule has no application to the internet communications involving port numbers. Port numbers are not voluntarily shared with any entity except the recipient at the other end of the transmission; like the person answering the telephone at the other end of your line. There is neither implied awareness of third parties with access to the communication information nor constructive relinquishment of the information.

To quote Bellovin again:

> "While there may be legal questions about whether people have a reasonable expectation of privacy in the TCP header fields, it is beyond dispute that such information is not normally given voluntarily to third parties."
>
> Id. at 43.

5 See Smith v. Maryland 442 U.S. 735 (1979) and United States v. Miller, 425 U.S. 435 (1976). For a full discussion of the doctrine, see Suppression, at 8 – 10.

6 "[T]here are two salient features of TCP. First, it contains port numbers. A port number is an address within a computer. If an IP address is similar to a building address, a port number more or less corresponds to a room within the building. … Second, the TCP header contains the information concerned with connection setup and maintenance."

Port numbers, like IP addresses, when constantly collected in real time for days and weeks can yield a detailed portrait of a person's on-line activity. They are akin to the "post-cut-through-dialed digits" ("PCD") from the telephony era. PCD were the extension numbers dialed after a connection was made to a main number. For example, extensions requesting entry of a credit account number, a social security number or date of birth. Some courts have held them to be content prohibited from collection under the Pen/Trap statute. See e.g. Bellovin, n. 356-357. For 51 years the law has recognized an expectation of privacy in the contents of one's conversation even in certain public areas. See Katz v. United States, 389 U.S. 347, 351, 88 S.Ct. 507 (1967)("[W]hat a person seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."). Port numbers, automatically selected and utilized by the inherent "communicative" selection process of internet transmission protocols, are *per se* the private contents of "conversation" utilized by every person who necessarily accesses the internet on a daily basis to meet the obligations of life in a digital age.

II. The Affidavit in Support of the Application for the Search Warrant Does Not Show Probable Cause and Could Only Have Been Allowed Because of the Magistrate Judge's Apparent Bias.

Background

Magistrate Judge Bowler heard the government's application for the issuance of the search warrant to seize and examine any and all computers, mobile devices, and related equipment and records on September 29, 2014. The affidavit alleged, in relevant part, as follows:

Allegations Regarding the DDOS Against BCH and the YouTube Video

- Boston Children's Hospital experienced a Distributed Denial of Service ("DDOS")

attack on April 20, 2014 against its public internet web page www.childrenshospital.org, IP address 134.174.13.5 which lasted until at least April 24, 2014. Exh. A to Suppression, ¶ 6.

- The incoming traffic, "originating from many IP addresses", Id., "resulted in significant disruptions to the BCH website and additional disruption to the network on which BCH and other Harvard University-affiliated hospitals communicate." Id. ¶ 8.
- "I [affiant FBI Special Agent Tunick] believe that the attack against BCH is related to an activist effort concerning the custody battle over teenage medical patient Justina Pelletier. This custody battle involved the Commonwealth of Massachusetts's taking custody of Justina Pelletier from her parents due to her serious medical condition." Id. ¶ 9.
- "On March 23, 2014 someone using the name "Shutdown Logan River Academy" posted a YouTube video entitled, "Anonymous #OpJustina Press Release Video. This video claimed to be from the hacking group Anonymous, was a call for action against BCH, and was accompanied by an online posting." Id. ¶ 10.
- The narration was by a computer-generated voice, "which states, among other things, that Anonymous or others with similar views "will punish all those held accountable and will not relent until Justina is free." Id. ¶ 11.
- Agent Tunick said, "…the imagery contained in the video is consistent with the group Anonymous. I know from my training and experience that the group Anonymous is known for numerous hacking attacks, many of which involve DDOS attacks." Id.
- The video voice said, "To the Boston Children's Hospital – why do you employ people that clearly do not put patient's [sic] first? We demand that you terminate Alice W.

Newton from her employment or you to [sic] shall feel the full unbridled wrath of Anonymous. Test us and you shall fail." Id. ¶ 12.

- The video posted a web address on the screen, "pastebin.com", "located at http://pastebin.com/tfew3Hn6, [which] lists detailed information about BCH, including:

  Name: Boston Children's Hospital

  Address: 300 Longwood Ave.

  Boston, MA 02115

  Website: www.childrenshospital.org

  IP Address: 134.174.13.5

  Server Type: Microsoft-IIS7.5" Id. ¶ 13.

- That "information is enough to implement or coordinate a DDOS attack, and the IP address listed in the posting, 134.174.13.5, is the IP address of BCH's server that was subsequently hit with the DDOS attack." Id. ¶ 14.
- Records for the account that posted the Youtube video "calling for the attack" show that it was "owned and managed by Martin S. Gottesfeld", and "was used to post this video on March 23, 2014 and log in to the account on April 1, 2014." Id. ¶ 16.
- RCN the cable company that controls that IP address lists Martin S. Gottessfeld as the customer assigned to that IP address from at least March 23 to April 1, 2014" and that "Gottesfeld receives his internet service at 28 Albion St., Apartment 1, Somerville, [MA]" Id. ¶ 17.
- Based on affiant's training and experience, "I know that this means that someone at the [28 Albion St., Apt. 1, Somerville, MA] used a computer, tablet, smartphone or,…. on

March 23, 2014 to post the YouTube video." Id. ¶18.

Allegations Concerning Defendant's Criticism of the Troubled Teen Industry and Other DDOS Attacks Associated with the Industry.

- After the BCH DDOS attack the FBI learned of other attacks against entities associated with BCH, the Justina Pelletier custody battle, or the troubled teen industry. Pertinently, these included Wayside Youth and Family Support Network, Greatschools.org and Logan River Academy. Id. ¶ 27.
- Gottesfeld allegedly had had direct email contact with Logan River Academy and Greatschools.org. Id. ¶ 28.
- In October, 2013 Gottesfeld sent an email to Logan River Academy informing the owner that a petition had been started on Change.org for Logan River Academy to stop the use of solitary confinement in its treatment of troubled youths. Id. ¶ 29.
- Logan River Academy experienced a DDOS attack in November, 2013 and its online records management service, BestNotes.com experienced a DDOS attack in March, 2014. Id.
- Gottesfeld has been linked to a Facebook account called "shutdownloganriver, a Twitter account named "stoploganriver" and a YouTube account called "shutdownloganriver, as well as maintaining a website named www.loganriver.com, all of which entities supposedly advocate shutting down Logan River Academy. Id. ¶ 30.
- "Gottesfeld sent an email in October 2013 asking that Greatschools.org, a website which lists rating[s] for various schools, no longer list Logan River Academy on its website. In this e-mail, Gottesfeld threatened that he would add Greatschools.org to his campaign

against Logan River Academy and would report the website to certain associations. Greatschools.org experienced a DDOS attack in July 2014." Id. ¶ 31.

Argument

A. Relevant Law.

The affidavit offered in support of the application for the search warrant did not demonstrate probable cause. This court's review of the question is *de novo.* Ornelas v. United States, 517 U.S. 690, 699,116 S.Ct. 1657 (1996). The information provided within the four corners of the affidavit must "warrant a man of reasonable caution in the belief that an offense has been or is being committed." Brinegar v. United States, 338 U.S. 160, 175-176, 69 S.Ct. 1302 (1949)(internal quotation marks omitted). "Probability is the touchstone." United States v. Khounsavanh, 113 F.3d 279,283 (1st Cir. 1997). "Probable cause exists when the affidavit upon which the warrant is founded demonstrates in some trustworthy fashion the likelihood that an offense has been or is being committed…" United States v. Shaefer, 87 F.3d 562, 565 (1st Cir. 1996)(internal quotation marks omitted). "[Mere] suspicion, rumour, or strong reason to suspect [wrong doing] are not sufficient." United States v. Vigeant, 176 F.3d 565, 569 (1999)(quoting United States v. Han, 74 F.3d 537, 541 (4th Cir. 1996)(citation omitted). A "warrant application must demonstrate probable cause that a particular person has committed a crime – 'the commission element'— and that enumerated evidence relevant to the probable criminality likely is located at the place to be searched – 'the "nexus" element.'" United States v. Zayas-Diaz, 95 F.3d 105, 110-111 (1st Cir. 1996).

The court's review must consider the "totality of the circumstances" and find a "substantial basis" for any conclusion that the affidavit meets the probable cause standard.

Illinois v. Gates, 462 U.S. 213, 231, 103 S,Ct. 2317 (1983).

B. As Applied in this Case.

The only relevant facts in the affidavit tending to show a connection between the defendant and the DDOS attack against Boston Children's Hospital are the information that he was critical of the 'troubled teen industry'; that a video posted on YouTube on March 23, 2014 was, in part, explicitly critical of Boston Children's Hospital's treatment of a teen age girl under its care; and that the video was uploaded from an IP address which had been assigned to the RCN router in defendant's residence in Somerville from March 23 to April 1, 2014 ¶¶ 9, 16-18.

At least one of the allegations contained in the affidavit was an opinion unsupported by apparently readily available factual verification. In paragraph 11, Agent Tunick states that he is familiar with Anonymous and that he knows that it,"is known for "numerous hacking attacks, including many DDOS attacks." He does not give any concrete, verifiable examples of such DDOS attacks by Anonymous, although one would think that, if so numerous, such examples would be readily available to him. Id. ¶ 11.

Several allegations are misleading. For example, Tunick states that the online posting, http//:pastebin.com/tfew3Hn6,that appeared at one point in the video, "is enough to implement or coordinate a DDOS attack, and the IP address listed in the posting, 134.174.13.5, is the IP address of BCH's server which was subsequently hit by the DDOS attack." But the actual link encountered through pastebin.com also includes the very publicly available mailing and website addresses of BCH which is consistent with the fact that earlier in the video, Anonymous asks viewers to express their protest against the unfairness and danger of Justina's confinement by writing letters and making phone calls. See video, at 1:57. Another example is found at ¶ 31,

where it is alleged that defendant "**threatened** that he would add Greatschools.org to his campaign against Logan River Academy and would report the website to certain associations." (emphasis supplied). This use of the verb "threatened" is misleading because it implies the use of a "strong arm", menacing warning or ultimatum. In fact, defendant's actual email was a direct, matter of fact, statement, a protest, if you will. He perceived Greatschools to be aiding and abetting a fraudulent and flagrantly abusive institution. He wanted them to rationally consider what they were doing by their support. In straightforward, non-threatening language he simply advised them:

> "If you continue to list Logan River Academy on your website, we will add greatschools.org to the petition [at Change.org, *supra*], and publicly urge you to delist them. We will also be sure that your name is mentioned publicly as marketing Logan River Academy and similar fraudulent and abusive programs."
>
> Exh. C, attached.

In addition, the affiant states that "This custody battle involved the Commonwealth of Massachusetts's taking custody of Justina Pelletier from her parents due to her serious *medical* condition." Id. ¶ 9 (emphasis supplied). This is misleading because the controversy was clearly not about Justina's medical condition, but the fact that Boston Children's Hospital, and a Massachusetts state agency and judge, had refused to consider her prior diagnosis of mitochondrial disease by competent medical personnel at Tufts Medical Center and, instead, had substituted a purely psychiatric diagnosis. This resulted in Justina's long-term confinement against her will and the termination of the parental rights of her mother and father by a state court. To omit the essence of the controversy and just call it a generic "medical condition" is misleading.

Most importantly, the language allegedly used in the video is protected speech. The

relevant passages are:

> "[the computerized-voice] which states, among other things, that Anonymous or others with similar views *"will punish all those held accountable and will not relent until Justina is free."* (italics supplied)
>
> Id. ¶ 11.

> And, "To the Boston Children's Hospital – why do you employ people that clearly do not put patient's [sic] first? We demand that you terminate Alice W. Newton from her employment *or you to [sic] shall feel the full unbridled wrath of Anonymous. Test us and you shall fail."* (italics supplied).
>
> Id. ¶ 12.

Neither of these passages involves "fighting words", a "clear and present danger" or a call to an imminent breach of the peace. If someone spoke them from the band box on the Boston Common in broad daylight to a packed crowd they would not be subject to arrest. In America one has the right to protest what he believes to be unlawful conduct. That includes conduct by an otherwise venerable and revered institution. The warnings are meant to sound an alarm. But they are not incitement to violence.

A fair reading of the affidavit does not demonstrate probable cause. For the sake of argument, without an admission, defendant recognizes that the magistrate could find that a crime was committed. A DDOS happened on or about April 20, 2014 at Boston Children's Hospital. But he asserts that there is insufficient evidence on the face of the affidavit to permit a reasonable person to find probable cause that <u>he</u> committed the alleged crime. There is no greater probability than not that the DDOS on April 20 was generated from a computer or other electronic device located at defendant's residence at 28 Albion Street, Apt. 1 in Somerville. There is nothing but conjecture that the DDOS of April 20 originated from defendant's computer, or indeed, from his residence. Most IP addresses used by residential customers

change from time to time. The affidavit acknowledges this fact by limiting its probability assessment to the uploading of the YouTube video on March 23, and setting the last date of use for that IP address as April 1, nineteen days before the alleged DDOS attack. Probabilities are understandably not exact but neither can they be predominantly speculative. "Probable cause exists when the affidavit upon which the warrant is founded demonstrates in some trustworthy fashion the likelihood that an offense has been or is being committed…" United States v. Shaefer, 87 F.3d 562, 565 (1st Cir. 1996)(internal quotation marks omitted). A "warrant application must demonstrate probable cause that a particular person has committed a crime – 'the commission element'." United States v. Zayas-Diaz, 95 F.3d 105, 110-111 (1st Cir. 1996). "[Mere] suspicion, rumour, or strong reason to suspect [wrong doing] are not sufficient." United States v. Vigeant, 176 F.3d 565, 569 (1999)(quoting United States v. Han, 74 F.3d 537, 541 (4th Cir. 1996)(citation omitted). In this case, defendant's advocacy against the troubled teen industry and Boston Children's Hospital in particular, may give rise to something more than 'mere suspicion' or 'rumour' that he was involved in the actual DDOS, but even 'strong reason to suspect wrong doing,', Vigeant, *supra*, is not sufficient for probable cause under the circumstances of this case. The motion to suppress should be allowed.

C. The Magistrate Judge's Appearance of Bias.

Background.

Magistrate Judge Bowler has strong personal and professional ties to Boston Children's Hospital, Harvard Medical School and the Wayside Youth and Family Support Network, ("Wayside"), all institutions involved in the present case although none is a party. Of course, BCH and Wayside were allegedly subjected to DDOS attacks. See ¶ ¶ 6 – 8, and ¶ 27

respectively. The affidavit presented to the magistrate for review on September 29, 2014 literally identified "Boston Children's Hospital" seven (7) times and its obvious representative abbreviation, "BCH", twenty-one (21) times. The fact that BCH is a "Harvard University-affiliated hospital" which sustained extensive damage in the DDOS' is explicit in paragraph 8 of the affidavit. Thus, there is little doubt that the magistrate was not aware of the possible conflict of interest.

Wayside provides both outpatient and secured residential treatment facilities in Framingham, Massachusetts for mental health counseling and family support services to children, young adults and families. www.waysideyouth.org/aboutus It is described as an "associated entity" of Boston Children's Hospital in the affidavit. ¶ 27. Both BCH and Wayside have received generous grants of money from The Boston Foundation, Exh. D, a premier philanthropic institution in Boston. Magistrate Judge Bowler was on the Board of Directors of The Boston Foundation from 1995 to 2004 and is currently a Director *Emeritis.* Exh. D. Wayside participates in the Giving Common, a fundraising portal sponsored by The Boston Foundation at https://givingcommon.org. Exh. E.

Boston Children's Hospital is a teaching hospital for Harvard Medical School. Magistrate Judge Bowler is married to Marc A. Pheffer, M.D., Ph.D. who is the Dzau Professor of Medicine at Harvard Medical School and a senior cardiologist at the Brigham & Women's Hospital, which is a Harvard Medical School affiliated hospital. Exh. F. Prior to starting her legal career Magistrate Bowler was a research assistant at Harvard Medical School. MB c.v. at https://www.scribd.com/document/138058835/Judge-Marianne-Bowler

Boston Children's Hospital claims approximately $600,000 in losses from the DDOS

attack it suffered.

Law

28 U.S.C. § 455(a) requires "[any] justice, judge or magistrate of the United States [to] disqualify himself in any proceeding in which his impartiality might reasonably be questioned."

> "This statute seeks to balance two competing policy considerations: first, "that courts must not only be, but seem to be, free of bias or prejudice." In re United States 158 F.3d 26, 30 (1st Cir. 1998)(quoting In re United States 666 F.2d 690, 694 (1st Cir. 1981)); and second, the fear that recusal on demand would provide litigants with a veto against unwanted judges, id."
>
> In re Boston's Children First, et al., Petitioners, 244 F.3d 164,167 (1st Cir. 2001).

But disqualification is only appropriate when a charge is supported by a factual basis. Id. At the same time the facts asserted must "provide what an objective, knowledgeable member of the public would find to be a reasonable basis for doubting the judge's impartiality." In re United States, 666 F.2d at 695. Although judges are allowed a "range of discretion" when deciding not to recuse, id. "we note that the district court should exercise that discretion with the understanding that, "if the question whether § 455(a) requires disqualification is a close one, the balance tips in favor of recusal." In re Boston's Children First, 244 F.3d at 168 (citing Nichols v. Avery, 71 F.3d 347, 352 (10th Cir. 1995)).

Relevant to the instant case, 28 U.S.C. 455(b) lists several situations which *require* a judge to disqualify him/herself:

> (b)(4) ...knowledge that a spouse has a financial interest…or any other interest that could be substantially affected by the outcome of the proceeding…
>
> (b)(5) He or his spouse …:
> (i) Is a party to the proceeding or an officer, director or trustee of a party
> (iii) Is known by the judge to have an interest that could be substantially affected by the outcome of the proceeding;…
>
> 28 U.S.C. § 455(b).

Judge Bowler recused herself from a case in 2017 with significant parallels to the present case. In Cabi, et al. v. Boston Children's Hospital, et al. she recused herself under both §§ 455(a) and 455(b)(4). Exh. G. Her stated grounds for recusal were that her "spouse, Marc A. Pheffer, M.D., Ph.D., is the Dzau Professor of Medicine at Harvard Medical School and a Senior Cardiologist at Brigham & Women's Hospital in Boston, a Harvard Medical School affiliated hospital." Additionally, she cited the fact that the plaintiffs were seeking discovery from the medical school which had, in turn, moved to quash the subpoena. Id. No reason was stated as the basis for noting § 455 (b)(4) as the additional grounds. But it perforce would have to be her knowledge that her spouse had "an interest, financial or otherwise, that could be substantially affected by the outcome of the case." Id.

The same grounds existed in the present case when Magistrate Bowler was presented with the application for a search warrant against the defendant Gottesfeld. Her husband, Dr. Pheffer's employer, Harvard Medical School, was just as likely to be dragged into the periphery of this case as in Cabi, et al. The discovery here certainly concerns the losses suffered by Boston Children's Hospital, the Harvard affiliated entity named as the principle victim in this case. That clearly would have given Dr. Pheffer an interest in the outcome of the case, one that the magistrate could not help be aware of, if only in a general sense.

But apart from the mandatory recusal, this case presented the magistrate with an obvious 'objective appearance of bias' that no reasonable member of the public would fail to notice: her personal connections to two Harvard Medical related entities (BCH, Brigham & Womens Hospital) the principle one of which, BCH, was the primary victim in the DDOS that gave rise to the application for the search warrant; her spouse's likely interest in the outcome of the case; and

herself as a director of The Boston Foundation a financial benefactor of both BCH and Wayside. Withal, it was error for Magistrate Bowler to hear the government's application for a search warrant for the defendant's residence in this case.

Defendant suggests that the error may be considered in two ways. First, as the magistrate could not be truly independent and neutral, therefore this court may consider that as a factor to weigh in its examination of the affidavit for probable cause. Second, should the court find no probable cause, there is no basis to apply the "good faith" exception to forgive the violation and permit the evidence. See United States v. Leon, 468 U.S. 897, 914 (1984)(citation omitted)("good faith exception" not applied in absence of "neutral and detached" magistrate); See also United States v. Decker, 956 F.2d 773, 778 (8th Cir. 1992)(good faith exception not applicable as issuing judge failed to act in neutral and detached manner).

For the reasons stated above, the defendant respectfully requests that all evidence obtained from the illegal search and seizure at his home at 28 Alpine Street, Apt. 1, Somerville, Massachusetts be suppressed and prevented from use at any trial herein.

DEFENDANT REQUESTS AN EVIDENTIARY HEARING ON THIS MOTION

Respectfully submitted,

MARTIN GOTTESFELD,

By his attorney,

/s/ Raymond E. Gillespie
Raymond E. Gillespie

BBO #192300
875 Massachusetts Avenue Suite 32
Cambridge, MA 02139
(617) 661-3222
rgillespie1@prodigy.net

Certificate of Service

I, Raymond E. Gillespie, hereby certify that a copy of this motion will be served on all parties registered to receive notice in this case as of March 20, 2018:

/s/Raymond E. Gillespie
Raymond E. Gillespie

031918 supp suppress